METHOD FOR ANALYSIS OF NETWORK

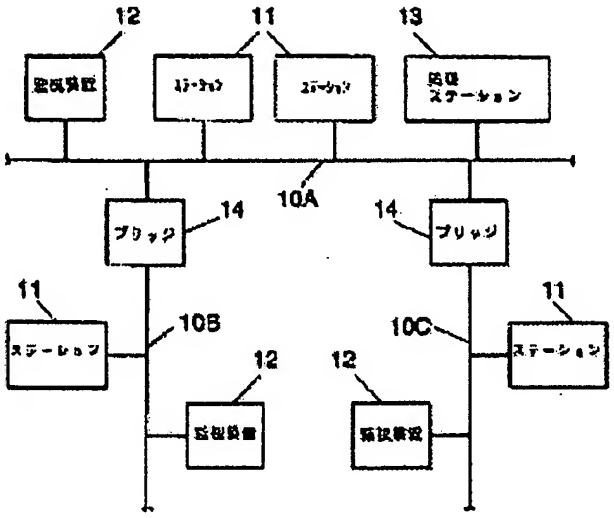
Publication number: JP7007518
Publication date: 1995-01-10
Inventor: NIIRU MATSUKII; PIITAA FUAARU; KORIN ROU
Applicant: HEWLETT PACKARD CO
Classification:
- international: ***G06F13/00; H04L12/26; H04L29/14;*** **G06F13/00; H04L12/26; H04L29/14;** (IPC1-7): H04L12/40; G06F13/00; H04L29/14
- European: H04L12/26
Application number: JP19940024293 19940222
Priority number(s): GB19930003527 19930222

Also published as:
EP0613270 (A2)
US5539659 (A1)
EP0613270 (A3)
EP0613270 (B1)

Report a data error here

Abstract of **JP7007518**

PURPOSE: To make easier the identification of an important data item regarding the management of a network by analyzing the data about the operating characteristics of network entities and sequentially studying the entities. CONSTITUTION: A monitor 12 collects the data about an entity traffic regarding the operation of a network during a fixed period. Then a central processing station 13 analyzes the data, forms an end set composed of at least one entity at one end of a sequence of entities, and stores the identity of each entity in the end set. The station 13 then identifies such an entity that exists in a newly generated end set, but does not exist in an extended hysteresis record, by comparing the entities in the newly generated end set with the entities existing in the extended hysteresis record by executing an analysis task containing this step on continuous N periods (where, N represents an integer of >1) and, then, on another period.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－7518

(43)公開日　平成７年(1995)１月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/40					
Ｇ０６Ｆ　13/00	３５３　Ｕ	7368－5Ｂ			
Ｈ０４Ｌ　29/14					
		7341－5Ｋ	Ｈ０４Ｌ　11/ 00	３２０	
		9371－5Ｋ	13/ 00	３１３	

審査請求　未請求　請求項の数１　ＯＬ　（全 9 頁）

(21)出願番号　特願平6－24293

(22)出願日　平成６年(1994)２月22日

(31)優先権主張番号　９３０３５２７．７

(32)優先日　1993年２月22日

(33)優先権主張国　イギリス（ＧＢ）

(71)出願人　590000400
ヒューレット・パッカード・カンパニー
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000

(72)発明者　ニール・マッキー
イギリス国ブリストル・ビーエス12・８エイダブリュ，ブラッドリー・ストーク，ザ・ヴェールズ・25

(72)発明者　ピーター・ファール
イギリス国ブリストル・ビーエス12・８エイダブリュ，ブラッドリー・ストーク，ザ・ヴェールズ・25

(74)代理人　弁理士　古谷　馨　（外２名）

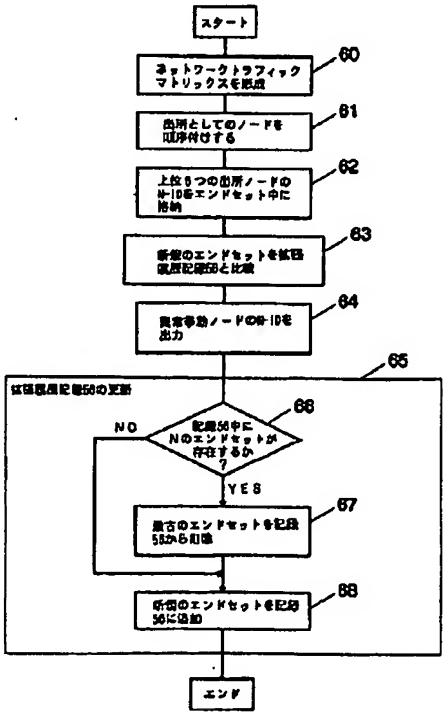
最終頁に続く

(54)【発明の名称】　ネットワーク解析方法

(57)【要約】

【目的】　ﾈｯﾄﾜｰｸの管理に関する重要なﾃﾞｰﾀ項目の識別を容易化すること

【構成】　関連するﾄﾗﾌｨｯｸを各々が有する複数のｴﾝﾃｨﾃｨを備えたﾈｯﾄﾜｰｸに関して用いられるﾈｯﾄﾜｰｸ解析方法であり、ﾈｯﾄﾜｰｸを監視して或る一定期間のﾈｯﾄﾜｰｸ動作に関するｴﾝﾃｨﾃｨのﾄﾗﾌｨｯｸについてのデータを収集し、或る順位にｴﾝﾃｨﾃｨを順序付けるｴﾝﾃｨﾃｨ動作特性に関して前記データを解析し、前記順位の一端の少なくとも1つのｴﾝﾃｨﾃｨからなるｴﾝﾄﾞｾｯﾄを形成し、そのｴﾝﾄﾞｾｯﾄの各ｴﾝﾃｨﾃｨの同一性を格納するというｽﾃｯﾌﾟを含む解析ﾀｽｸを有する。この解析ﾀｽｸが、連続するNの期間（Nは1より大きい整数）について、次いで更なる期間について実行されて、結果的に新規に生成されたｴﾝﾄﾞｾｯﾄ中のｴﾝﾃｨﾃｨが前記拡張履歴記録中のｴﾝﾃｨﾃｨと比較されて、新規に生成されたｴﾝﾄﾞｾｯﾄ中には存在するが前記拡張履歴記録中には存在しないあらゆるｴﾝﾃｨﾃｨ（異常挙動ｴﾝﾃｨﾃｨ）が識別される。



1

【特許請求の範囲】

【請求項1】関連するトラフィックを各々が有する複数のエンティティを備えたネットワークに関連して用いられるネットワーク解析方法であって、この方法が、ネットワークを監視して或る一定期間のネットワーク動作に関するエンティティのトラフィックについてのデータを収集し、或る順位にエンティティを順序付けるエンティティ動作特性に関して前記データを解析し、前記順位の一端における少なくとも1つのエンティティからなるエンドセットを形成し、そのエンドセットを構成するエンティティまたは各エンティティの同一性を格納する、というステップを含む解析タスクを有し、また前記方法が、

(1) 連続するNの前記期間について前記解析タスクを実行し（ここで、Nは1より大きい整数）、これにより、前記N期間について前記エンドセット中のエンティティに関する拡張履歴記録を形成し、

(2) 更なる前記期間について前記解析タスクを実行し、これより新規に生成されたエンドセット中のエンティティを前記拡張履歴記録中のエンティティと比較し、これにより、新規に生成されたエンドセット中には存在するが前記拡張履歴記録中には存在しないあらゆる異常挙動エンティティを識別する、

というステップを含むことを特徴とする、ネットワーク解析方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、トラフィックの送信および／または受信を行うように動作する複数のノードを備えたネットワークに関連して用いるためのネットワーク解析方法に関するものである。

【0002】

【従来の技術】ネットワーク監視システムがより精巧かつ広範なものになるにつれ、そのような監視システムにより提供されるネットワーク性能についての多くのデータ中で重要なデータを識別することに関する問題がネットワークのオペレータにとって増大してきている。

【0003】

【発明が解決しようとする課題】本発明の目的は、ネットワークの管理に関する重要なデータ項目の識別を容易化することにある。

【0004】

【課題を解決するための手段】本発明の一態様によれば、関連するトラフィックを各々が有する複数のエンティティを備えたネットワークに関連して用いるためのネットワーク解析方法が提供される。この方法は、ネットワークを監視して、或る一定期間のネットワーク動作に関するエンティティのトラフィックについてのデータを収集し、或る順位にエンティティを順序付けるエンティティの動作特性に関して前記データを解析し、前記順位

2

の一端における少なくとも1つのエンティティからなるエンドセットを形成し、そのエンドセットを構成する各エンティティの同一性を格納する、というステップを含む解析タスクを有するものであり、また前記方法は、

(1) 連続するNの前記期間について前記解析タスクを実行し（ここで、Nは1より大きい整数）、これにより、前記N期間について前記エンドセット中のエンティティに関する拡張された履歴記録（以下、拡張履歴記録と称す）を形成し、(2) 更なる前記期間について前記解析タスクを実行し、これにより新規に生成されたエンドセット中のエンティティを前記の拡張履歴記録中のエンティティと比較し、これにより、あらゆるエンティティ（ここでは異常な挙動をしたエンティティ（以下、異常挙動エンティティと称す）、即ち、新規に生成されたエンドセット中には存在するが前記記録中には存在しないエンティティ）を識別する、というステップを含むものである。

【0005】考察対象となるネットワークエンティティは通常はネットワークノードである。しかし、そのエンティティは、ノード対、論理セグメント、セグメント対、外部の宛先、または、ネットワークに関連する他の適当な分類の資源とすることが可能なものである。

【0006】解析タスクは、例えば、1時間にわたるネットワークトラフィックの監視操作を含むことが可能であり、この操作が2週間(N=14)にわたりステップ(1)で毎日繰り返されて、拡張履歴記録が導出される。この記録は、ネットワークの正常な挙動を効果的に包含するものである。この解析タスクの再実行の際に（ステップ(2)）、順位付けされたエンドセット中に新規なエンティティが現れた場合には、何らかの異常なネットワーク挙動が発生したものと合理的に仮定することができ、その異常挙動エンティティの同一性により、ネットワークのオペレータの注意を喚起することができる。

【0007】好適には、本発明の方法は、ステップ(2)の続行を基礎として、例えばステップ(2)を毎日行って実施される。勿論、ネットワークは一般に動的な性質を有するものであり、その正常な挙動パターンは時間と共に変化する。従って、拡張履歴記録が、継続実行を基礎として更新されるのが好適である。このため、本発明の好適実施例によれば、ネットワーク解析方法のステップ(2)は、更に以下のステップを含むものとなる。即ち、前記異常挙動エンティティの識別後に、拡張履歴記録により網羅されるNの期間のうち最も古いものに関連するエンドセット中に存在することを理由として、その拡張履歴記録中に存在するエンティティをステップ(2)で新規に生成されたエンドセットのエンティティと置換することにより拡張履歴記録の更新を行う、というステップである。ここで、前記ステップ(2)は、連続する前記の各期間について繰り返され、これにより、継続実行を基礎として前記異常挙動エンティティが識別されることに

なる。

【０００８】好適には、該ネットワーク解析方法は、異常挙動エンティティを探索に２つ以上の計測を用いる。この場合、その解析タスクは、複数の異なる前記動作特性に関するトラフィックデータを解析するよう動作し、個々の拡張履歴記録は前記の各動作特性に関連付けして保持され、これにより、前記動作特性のいずれに関しても異常挙動エンティティを識別することが可能となる。

【０００９】考察中のエンティティがネットワークノードである場合、前記解析タスクにより形成される前記エンドセットは、好適には以下のうちの１つとなる。

【００１０】

－　トラフィックに関する上位出所ノード
－　トラフィックに関する上位宛先ノード
－　上位サーバノード
－　上位クライアントノード
－　ブロードキャストに関する上位出所ノード
－　マルチキャストに関する上位出所ノード

以下、本発明によるネットワーク解析方法を、非限定的な例により図面を参照して説明することとする。

【００１１】

【実施例】図１に例示する典型的なローカルエリアネットワークでは、複数のステーション11,12,13がケーブルセグメント10A,10B,10Cを介して相互に接続されている。そのネットワークは、ケーブルセグメント10B,10Cをケーブルセグメント10Aにそれぞれ接続するブリッジ（スパン装置）14により３つの論理セグメント（レベル2サブネットワーク）に分割されている。当業界で周知のように、それらのブリッジは、ネットワークセグメント間を通過するトラフィックのフィルタリングを行う働きをするものであり、これにより、特定セグメントから発せられて同一セグメント（ローカルトラフィック）上の１ステーションに向かうメッセージが、単一または複数のブリッジ14を介して他のセグメントへと送られることがなくなる一方、或るセグメントで発せられて他のセグメント（非ローカルトラフィック）に向かうメッセージは前記ブリッジを横切ることが可能となる。ステーション11,12,13は、ブリッジ14と共にネットワークのノードを構成する。

【００１２】この例示のローカルエリアネットワークにおいて、ステーション11,12,13間のメッセージは、ネットワークを介してブロードキャストされるパケット（フレームとも呼ばれる）といった形態で伝送される。典型的には、１つのパケットは、図２で例示された形態を有するものであり、出所アドレス（パケットを送出するステーションのアドレス）および宛先アドレス（パケットの受信を意図するステーションのアドレス）を含むパケットヘッダ15と、受信側ステーションに送られるべきデータを含み、通常はエラーチェックコードを含む情報フィールド16とを有している。また、使用する特定のパケット形式に依存して、別のフィールドを存在させることも可能である。従って、例えば、パケットヘッダおよび情報フィールドの双方を網羅するCRC（サイクル冗長性チェック）フィールドを存在させることも可能である。

【００１３】図１のネットワークは、例えば、当業者に周知のEthernetネットワークとすることが可能なものである。

【００１４】図１のネットワークは、複数の監視装置（ステーション12）および中央処理ステーション13からなるネットワーク監視システムにより監視されるように構成されたものである。その監視装置の各々は、そのネットワークのサブネットワークのそれぞれの１つと関連するものである。各監視装置は、その関連するサブネットワーク上のパケットをランダムにサンプリングし、そのサンプリングされたパケットに関するデータを収集されたデータパケット（以下、収集データパケットと称す）という形で処理ステーション13に戻すよう動作する。このデータは、サンプリングされたパケットの出所ノードアドレスおよび宛先ノードアドレスを少なくとも含むものである。適当なサンプリング式監視システムは、本出願人によるヨーロッパ特許出願EP-A-0480555明細書で説明されている。以下で明らかになるように、監視システムの性質は（特に、それがサンプリング式システムであるか否かを問わず）、そのシステムがネットワークを横切るトラフィックに関する適切なデータを収集できるものであれば、本発明にとって重要なものではない。

【００１５】監視装置12によりネットワークを介して送出された収集データパケットを受信すると、処理ステーション13は、それらのパケットを格納して、後続の処理および解析を実施する。

【００１６】その処理ステーション13は、例えば、適当なネットワークインタフェース（図示せず）を介してネットワークとインタフェースをとる標準的なワークステーションにより構成される。このようなワークステーションには、作業用データおよびプログラムセグメントを格納するためのRAMメモリや、プログラムの永久的な格納のためのROMメモリや、前記RAMメモリに保持されているデータを前記プログラムに従って処理するためのプロセッサや、種々の入出力装置が、標準的な態様で設けられる。それら要素はいずれも標準的なものであり、当業者に周知のものであるので、ここでは、その例示または説明を省略することとする。

【００１７】処理ステーション13は、ネットワークセグメントおよびノードのリストを維持するものであり、また、既知の態様で動作してネットワークに関するトラフィックマトリクスを生成するものである。図３は、その目的のために処理ステーション13により保持されるメインデータ構造を示すものであり、特に、以下のものが保持される。

【００１８】・サブネットワークリスト51
これは、ネットワークの全ての既知のサブネットワーク（論理セグメント）のリストであり、その各サブネットワークは、サブネットワーク同一性SN-IDと、第１ポインタTM-POINTERと、第２ポインタN-POINTERとを格納するフィールドを含むエントリをそれぞれ有している。

【００１９】・ノードステーションリスト52
これは、ネットワークの全ての既知のノードのリストであり、その各ノードは、ノード同一性N-IDおよびポインタNEXT N-POINTERを格納するフィールドを含むエントリをそれぞれ有している。いずれかの特定のサブネットワークに関連付けされるべき第１ノードは、サブネットワークリスト51中の対応するサブネットワークエントリのN-POINTERをセットすることにより前記特定のサブネットワークに関連付けされて、ノードリスト52中の適当なノードエントリを指すことになる。それと同じサブネットワークとの更なるノードの関連付けは、そのサブネットワークと関連付けされた最後の先行ノードのNEXT N-POINTERを用いて、そのサブネットワークと関連付けされるべき次のノードのエントリを指すことにより達成され、これにより、リンクされたノードリストが構築される。

【００２０】・ネットワークトラフィックマトリクス53
これは、ネットワークに関するトラフィックマトリクスデータを保持するために形成されたアレイである。図４に例示の典型的なトラフィックマトリクスは、各々の出所ノード／宛先ノードの対に、所与の時間間隔においてネットワークにより搬送されるパケットの数を与えるものである（同図では異なる各ノード11は11A,11B,11C,...11Nで示されている）。各サブネットワーク毎に部分的なトラフィックマトリクスを形成することも可能であり、この場合には、適当なポインタTM-POINTERをサブネットワークリスト51中に保持することができる。

【００２１】処理ステーション13により収集および処理がなされたトラフィックデータは、ネットワークに関連させた様々な資源または資源のグループ化の順位付けのために用いることができる。従って、例えば、ネットワークの各ノードを、それらが発するトラフィックの量、または、それらが受信するトラフィックの量によって順位付けすることができる。同様に、ネットワークの論理セグメントを、それらが発する、または、それらが受信する情報の量によって順位付けすることができる。同様に、各ノード対または各セグメント対を、それらが発しまた受信するトラフィックの量に従って順位付けすることができる。この例の場合、別の順位付けを同様に良好に用いることができるが、各ノードが発するトラフィックの量によるノードの順位付けに関しては考察を行うこととなる。

【００２２】実際には、そのような順位付けの一端または他端に現れるノードのみに関心が生じるのが一般的であり、例えば、ノードが発するトラフィックによるそのノードの１つの順位付けにおける上位５ノードまたは最後の５ノードのいずれかのみに関心が生じる。ネットワークトラフィックマトリクス53が与えられた場合、そのマトリクスを詳しく調査して、例えば上位５つの出所を識別し、そのノードの同一性を図５に示すような適切なエンドセットデータ構造55中に記録することは比較的簡単である、ということが理解されよう。本発明のネットワーク解析方法は、順位付けされたエンドセット情報を用いて拡張履歴記録を構成する。この拡張履歴記録は、正常なネットワークの挙動を提供する働きをするものであり、その挙動に対して、現在の挙動の判定を行うことが可能となる。図６を参照して一層詳細に説明すると、本発明の好適実施例では、ネットワークの性能についてトラフィックデータが毎日収集されて、ネットワークトラフィックマトリクスを生成するために用いられる（ステップ60）。その後、そのトラフィックマトリクスが検査されて上位５つの出所ノードが識別され（ステップ61）、それらノードの同一性が１つのエンドセットデータ構造55に入力される（ステップ62）。

【００２３】Nの先行して生成されたエンドセットデータ構造55は、処理ステーション13によって保持され、これらのNのエンドセットが、順位付けステップ61のネットワーク動作特性の主体に関する履歴記録56を形成している。ルーチンのステップ63では、最近に生成されたエンドセットデータ構造55中のノードの同一性が、拡張履歴記録56を形成するデータ構造55中のノードの同一性と比較される。新規に生成されたエンドセットデータ構造55が、履歴記録には存在しない単一または複数のノードを含んでいる場合には、それらノードの同一性が、ネットワークのオペレータによる考察のために出力される（ステップ64）。ここで、そのようなノードは、考察中のエンドセットで最近に現れなかったものであるので、「異常な挙動をした」ノードとして分類される。

【００２４】図６のルーチンのステップ65は、最も古いエンドセットデータ構造55を除去して（サブステップ67）それを新規に生成されたものと置換する（サブステップ68）ことにより拡張履歴記録を更新する、というステップを含むものである。このようにして、変化するネットワーク挙動に拡張履歴記録が適合する。

【００２５】勿論、Nのエンドセットデータ構造55が拡張履歴記録中に配置されるまで、最も古いエンドセットは削除されるべきでなく、これは、サブステップ66で実行されるテストにより処理される。

【００２６】図６のルーチンを毎日実行させることにより、オペレータに異常挙動ノードが通知されると同時に、拡張履歴記録が連続して更新されることになる、ということが理解されよう。図６のルーチンは、好適には、１日を基礎として自動的に実行されるよう構成される。Nの値は、例えば14となる。

7

【0027】本発明の方法は、同じトラフィックデータ（例えば、上位の出所および上位の宛先に対するもの）から導出される幾つかの異なる順位付けに適用可能である、ということが理解されよう。更に、これらの順位付けは、同じタイプのネットワークの資源または資源のグループ化に適用する必要性のないものである。従って、その順位付けは、（トラフィック量の観点から）上位の出所ノードおよび上位のセグメント対に関して適用することができる。更に、考えられるセキュリティ破壊を示唆する異常な外部通信を、上位の宛先での変動が示すことがあるので、外部の宛先の上位について順位付けを行うこともできる。

【0028】上述では、順位付けは、単に、伝送されたパケットの数に基づいて行われるトラフィック測定値に関して実施されている。実際に、或る順位付けの場合には、更に簡単な計測として、関係のあるノード（または他のネットワーク資源もしくは資源をグループ化したもの）と、そのノードからトラフィックを受信しまたはそのノードへトラフィックを送信するそのノードと対等なものの数とに関してカウントを行う、というものがある。しかし、監視システムが所要のデータを収集するよう好適に適合されている場合には、一層高度なトラフィック測定値（例えば、伝送されたバイトの数）を用いることも可能である、ということが当業者には理解されよう。更に、パケットの情報フィールドの中容を調べることにより、一層高度の情報を得ることができる。従って、そのような情報から、出所ノードがサーバとして動作しているかクライアントとして動作しているかを判断して、その分類を順位付けの判定基準（即ち、例えば上位サーバ）として用いることが可能である。例えば、TCP/IPプロトコルスーツに従って動作している際にその出所ポートが「周知のポート」である場合には、ノードは上記のようにしてサーバとして分類される。考えられる他の順位付けの判定基準には、ブロードキャストの出所およびマルチキャストの出所のための上位ノードが含まれる。

【0029】既述のように、上記説明のネットワーク解析方法は、ノード等の単一資源と同様に、資源をグループ化したものからなるネットワークエンティティにも適用可能である。そのようなグループ化したものは、サブネットワーク、または、ノードもしくはサブネットワークの対を含むことができる。「サブネットワーク」とは、7層OSI参照モデルのレベル2のブリッジにより実行されるネットワークの細分化だけでなく、スパン装置によるネットワークの他のあらゆる細分化（例えば、ルータにより実行されるレベル3での細分化等）によるものも意味している。

【0030】Nの値、収集期間、および監視反復率は全て、上記説明のものから変更可能であることが理解されよう。

8

【0031】以下に、本発明の実施態様を列挙する。

【0032】1.関連するトラフィックを各々が有する複数のエンティティを備えたネットワークに関連して用いられるネットワーク解析方法であって、この方法が、ネットワークを監視して或る一定期間のネットワーク動作に関するエンティティのトラフィックについてのデータを収集し、或る順位にエンティティを順序付けるエンティティ動作特性に関して前記データを解析し、前記順位の一端における少なくとも1つのエンティティからなるエンドセットを形成し、そのエンドセットを構成するエンティティまたは各エンティティの同一性を格納する、というステップを含む解析タスクを有し、また前記方法が、(1) 連続するNの前記期間について前記解析タスクを実行し（ここで、Nは1より大きい整数）、これにより、前記N期間について前記エンドセット中のエンティティに関する拡張履歴記録を形成し、(2) 更なる前記期間について前記解析タスクを実行し、これより新規に生成されたエンドセット中のエンティティを前記拡張履歴記録中のエンティティと比較し、これにより、新規に生成されたエンドセット中には存在するが前記拡張履歴記録中には存在しないあらゆる異常挙動エンティティを識別する、というステップを含むことを特徴とする、ネットワーク解析方法。

【0033】2.前記異常挙動エンティティの識別後に、前記拡張履歴記録により網羅されるNの期間のうち最も古いものに関連するエンドセット中に存在することを理由として、その拡張履歴記録中に存在するエンティティを前記ステップ(2)で新規に生成されたエンドセットのエンティティと置換することにより拡張履歴記録の更新を行う、というステップを前記ステップ(2)が更に含み、このステップ(2)を連続する前記期間について繰り返し、これにより継続実行を基礎として前記異常挙動エンティティを識別することを特徴とする、前項1記載の方法。

【0034】3.前記解析タスクが、複数の異なる前記動作特性に関するトラフィックデータを解析し、前記ステップ(1)が、前記の各動作特性に関して前記拡張履歴記録をそれぞれ保持するように動作し、前記ステップ(2)が、少なくとも1つの前記動作特性に関するものとして識別されたあらゆるエンティティを異常挙動エンティティとして識別する、ということを特徴とする、前項1または前項2記載の方法。

【0035】4.前記の各エンティティがネットワークのノードであることを特徴とする、前項1または前項2記載の方法。

【0036】5.前記解析タスクにより形成される前記エンドセットが、

トラフィックに関する上位出所ノード

トラフィックに関する上位宛先ノード

上位サーバノード

9　　10

上位クライアントノード
ブロードキャストに関する上位出所ノード
マルチキャストに関する上位出所ノード
のうちの1つであることを特徴とする、前項4記載の方法。

【0037】6.前記の各エンティティがネットワークのノードの対であることを特徴とする、前項1または前項2記載の方法。

【0038】7.前記の各エンティティがネットワークのサブネットワークであることを特徴とする、前項1または前項2記載の方法。

【0039】8.前記の各エンティティがネットワークのサブネットワークの対であることを特徴とする、前項1または前項2記載の方法。

【0040】9.前記の各サブネットワークがネットワークの論理セグメントであることを特徴とする、前項7または前項8記載の方法。

【0041】10.前記の各エンティティがネットワークの外部の宛先であることを特徴とする、前項1または前項2記載の方法。

【0042】11.前記解析タスクにより形成された前記エンドセットが上位通信エンティティを表すものであることを特徴とする、前項6ないし前項10のいずれかに記載の方法。

【0043】

【発明の効果】本発明は上述のように構成したので、ネットワークの管理に関する重要なデータ項目の識別を容易化することが可能となる。

【図面の簡単な説明】

【図1】本発明の方法による解析のためにトラフィックデータを収集するネットワーク監視システムを形成するように1つの処理ステーションおよび多数の監視装置が接続されているネットワーク全体を示すブロック図である。

【図2】図1のネットワークを介して伝送されるデータパケットの一般形態を示す説明図である。

【図3】サンプリング式監視装置からのデータの処理において図1の処理ステーションにより用いられる或るデータ構造を示す説明図である。

【図4】図1のネットワークに関するトラフィックマトリクスの一例を示す表である。

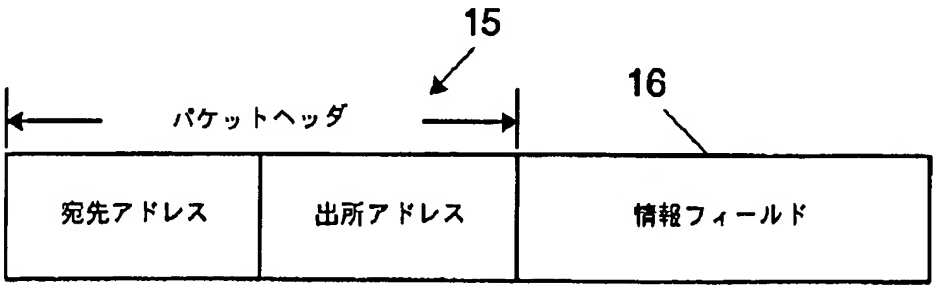
【図5】拡張履歴記録を形成する「上位5つの出所」のデータ構造の収集を示す説明図である。

【図6】本発明のネットワーク解析タスクを実施するルーチンを示すフローチャートである。

【符号の説明】

11　ステーション
12　監視装置
13　中央処理ステーション
51　サブネットワークリスト
52　ノードステーションリスト
53　ネットワークトラフィックマトリクス
55　エンドセットデータ構造
56　拡張履歴記録

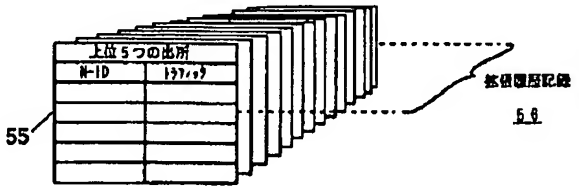
【図2】



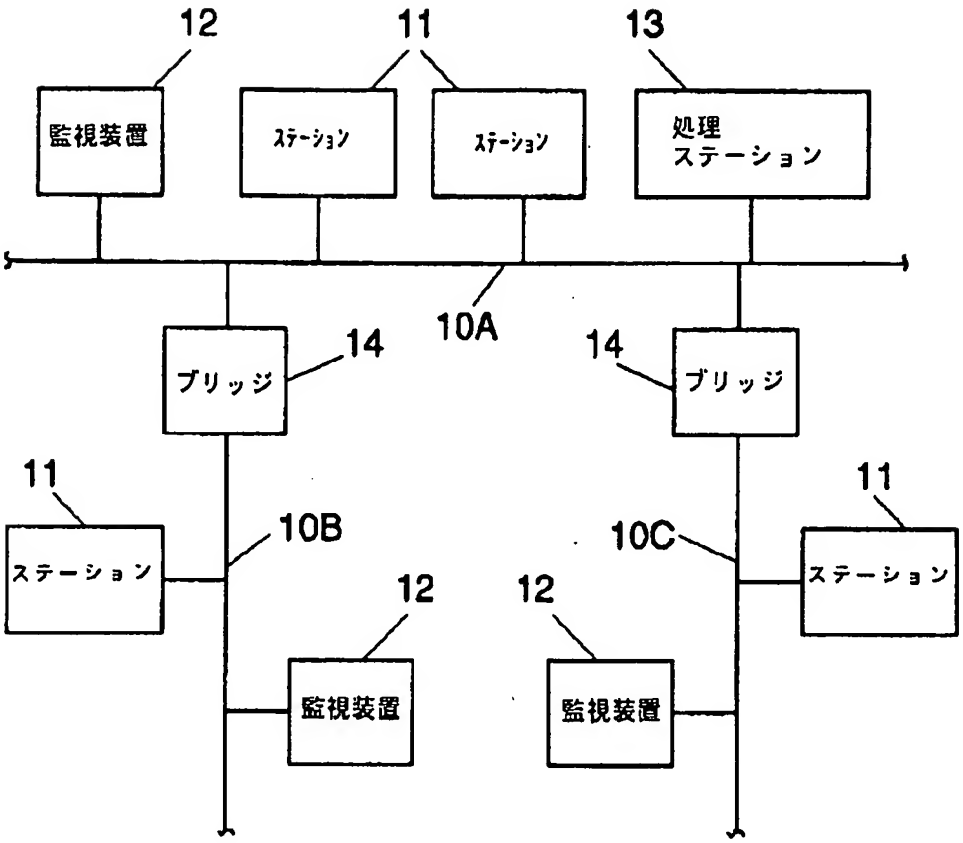
【図4】

ネットワークトラフィックマトリクス		宛先ノード 11A	11B	11C	----- 11N
出所ノード	11A	-	21	9	65
	11B	42	-	100	100
	11C	69	84	-	15
	⋮				
	11N	150	29	75	-

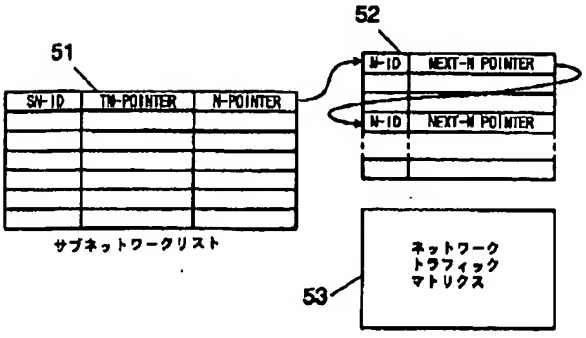
【図5】



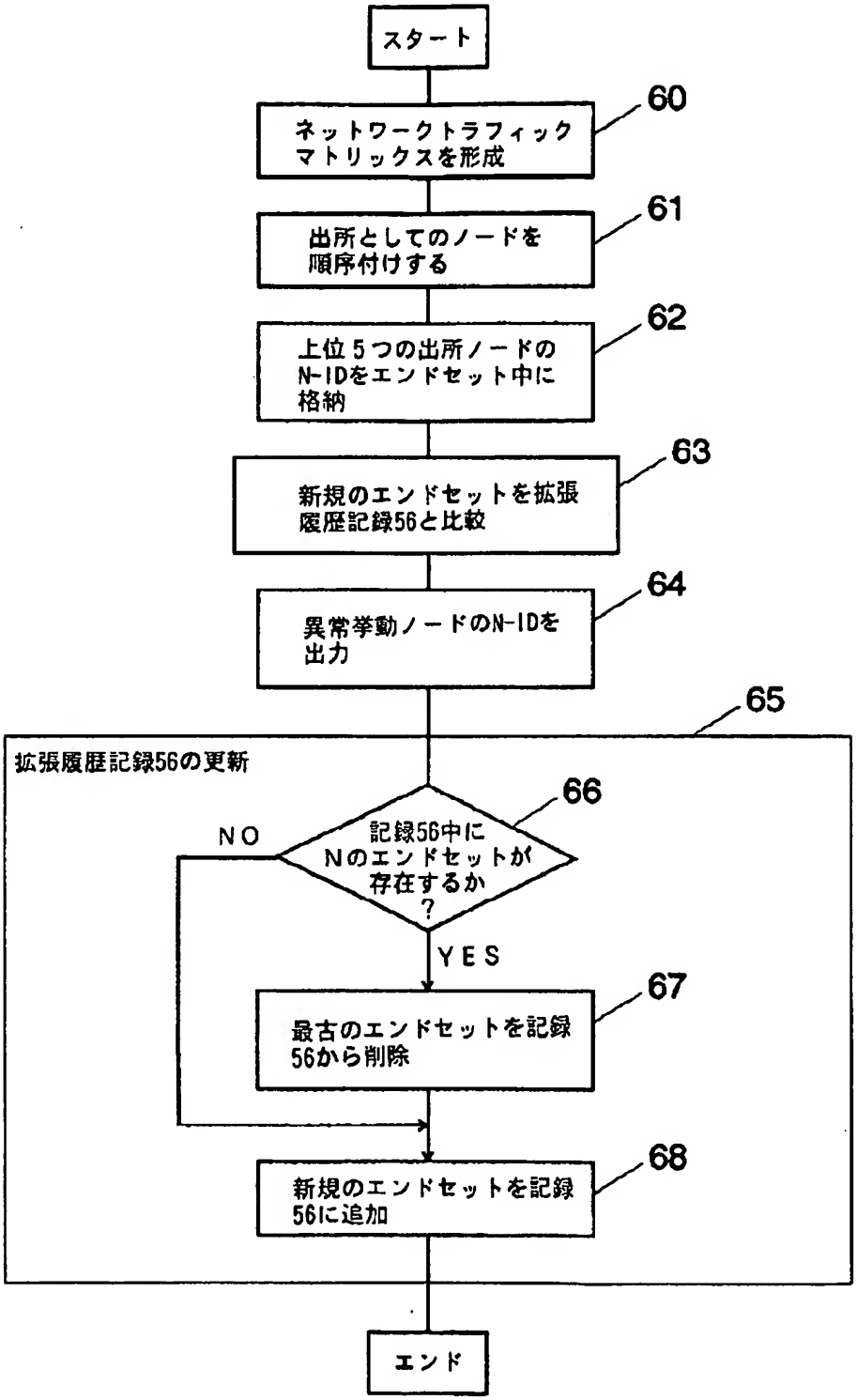
【図1】


12
11
13
監視装置
ステーション
ステーション
処理
ステーション
10A
14
14
ブリッジ
ブリッジ
11
11
10B
10C
ステーション
ステーション
12
12
監視装置
監視装置

【図3】


51
52
SN-ID
TN-POINTER
N-POINTER
N-ID
NEXT-N POINTER
N-ID
NEXT-N POINTER
サブネットワークリスト
ネットワーク
トラフィック
マトリクス
53

【図6】


スタート
ネットワークトラフィック
マトリックスを形成
60
出所としてのノードを
順序付けする
61
上位５つの出所ノードの
N-IDをエンドセット中に
格納
62
新規のエンドセットを拡張
履歴記録56と比較
63
異常挙動ノードのN-IDを
出力
64
65
拡張履歴記録56の更新
66
記録56中に
Nのエンドセットが
存在するか
？
NO
YES
最古のエンドセットを記録
56から削除
67
新規のエンドセットを記録
56に追加
68
エンド

フロントページの続き

(72)発明者　コリン・ロウ
イギリス国グロスターシャー・ジーエル
12・7エルティ，ウォットン－アンダー－
エッジ，パークランズ・19